



Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation

September, 2010

Agenda

- Triumfant Introduction
- SCAP Implementation Basics
- Security Configuration Management
- Vulnerability Scanning
- TNC Implementation



Introduction to Triumfant

Triumfant is an endpoint security and configuration management solution that is differentiated by the ability to:

- Use change detection coupled with patented analytics to detect the malicious activity that evades other defenses
- Build a surgical and contextual remediation to address detected problems
- Continuously enforce configurations and policies
- Deliver fine-grained reporting and analytics against the endpoint population with minimal intrusion



Why Triumfant is Different

Differentiator	Why It Matters
Change detection triggers analysis	Eliminates need for prior knowledge, makes detection attack agnostic
Deep, continuous monitoring	Assumes nothing, monitors everything, detects all changes
Contextual Analytics	Critical intel to analyze attacks, correlate all damage, and build a remediation
Automated Remediation	Eliminates coding and re-imaging, continuous enforcement
Donor Technology	Addresses the missing/corrupted attribute problem by turning the pop. into a donor

How it Works

Continuously scans for changes

- Elemental indicator of problems or attacks
- Eliminates need for prior knowledge
- Immediately triggers analysis for suspected malicious attacks

Analyzes detected changes

- Builds and then leverages learned context of broader population
- Categorizes: benign, anomalous, malicious
- Correlates changes into broader incidents

Takes appropriate action

- Builds a remediation for each incident
- Creates alerts, powers situational awareness
- Integrates with other tools in the ecosystem



Triumfant and SCAP

- Early mover in SCAP integration
- Third (or so) product NIST SCAP FDCC Validated Scanning Tool
- Only tool with fully automated remediation
- Strikes balance between performance and data currency

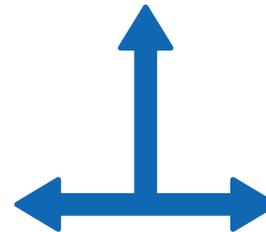


Overview of the Architecture

Endpoint



Server



Continuous Scanning to the Granular Level

Endpoint



Thin, efficient agent

- Scans, executes remediations, communicates w/server
- Small footprint: 25 Mb, < 1% of CPU, no stored information
- Minimal network traffic
- Hardened and protected
- Includes OVAL interpreter

Scans 200k+ attributes:

- Registry keys
- Files – MD5 hash
- Processes
- Services
- Event Logs
- Performance counters
- Security settings
- Hardware attributes
- Memory tables



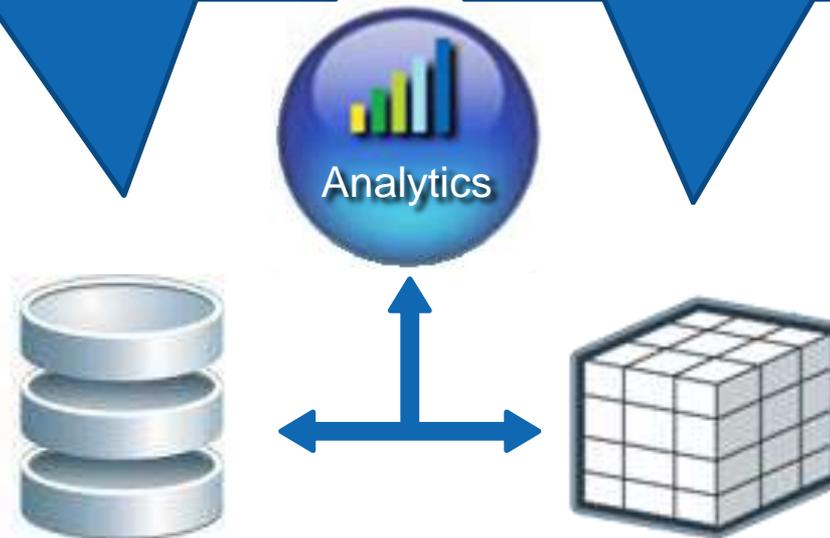
A Unique View of the Population

The data repository

- Most comprehensive endpoint attribute repository
- Maximum 24 hour latency
- Change data capture
 - Minimizes intrusion on endpoint
 - Minimizes network impact

The Adaptive Reference Model

- Multi-dimensional model of the endpoint population
- Automatically synthesized
- Continuously learns and adapts
- Normative baseline of all data



Configuration Management

Configuration checks are converted to Triumfant policies

- Comes out-of-the-box with policies
- Admin enables policies per population or per groups of machines
- Uses the attributes gathered in the normal scan scope

Two parts to the policy

- The actual pass/fail configuration test
- The data required to power the Triumfant remediation process
- Some specialized remediation processes – rename Admin, rename Guest

Configuration results evaluated as part of normal process

- Violations noted
- Remediation constructed using donor technology as needed



Flexible Reporting

The screenshot displays the Triumphant Resolution Manager web application. The main interface shows a navigation pane on the left and a central area with several summary reports. A detailed report for 'FDCC-Windows-XP Exceptions (155)' is overlaid on the right side of the screen.

FDCC-Windows-XP Exceptions (155)

Count	Rule Name	Result
2	() security_patches_up_to_date	fail
2	(CCE-1909-1) edlin.exepermissions	fail
2	(CCE-1916-6) netsh.exepermissions	fail
2	(CCE-1937-2) tintsvr.exepermissions	fail
2	(CCE-1978-6) denyaccessfromnetwork-gu...	fail
2	(CCE-2052-9) arp.exepermissions	fail
2	(CCE-2100-6) auditlogonevents	fail
2	(CCE-2145-1) eventcreate.exepermissions	fail
2	(CCE-2173-3) prohibit_installation_network...	fail

FDCC-Windows-Vista Exceptions (3)

Count	Rule Name	Result
1	() security_patches_up_to_date	fail
1	(CCE-3380-3) named-pipes-accessed-ano...	fail
1	(CCE-3452-0) registry_policy	fail

FDCC-XP-Firewall Exceptions (24)

Count	Rule Name	Result
2	() security_patches_up_to_date	fail
2	(CCE-2476-0) allow_remote_administration...	fail



Vulnerability Scanning

1. Vulnerability data extracted from MITRE database
 2. OVAL content packaged with XCCDF, sent to agent
 3. OVAL interpreter on agent runs scan
 4. Results placed in associated registry key
 5. Registry key scanned in normal processing
 6. Changes noted, sent to server for analysis
 7. Scan results tied back to CVEs at server level
- Fine grain control allows for specific criteria sets for specific groups
 - Comes out of the box with SCAP reports
 - Options to set alerts for violations



Vulnerability Analysis

Triumfant continuously scans for vulnerabilities

- Scans at the agent level, so it confirms the vulnerability – other tools can tell you if you ***might*** have a vulnerability
- Very efficient
 - Only returns data to the server when changes are detected
 - Minimizes impact on machine, network and server

A wealth of available data

- Vulnerability reporting without impacting the endpoints
- Vulnerability data even if the machine is offline
- Enables correlation analysis between attacks and vulnerabilities
- Significantly reduces re-imaging (6-12 month ROI)



Trusted Network Connect

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing

Open Standards for Network Security

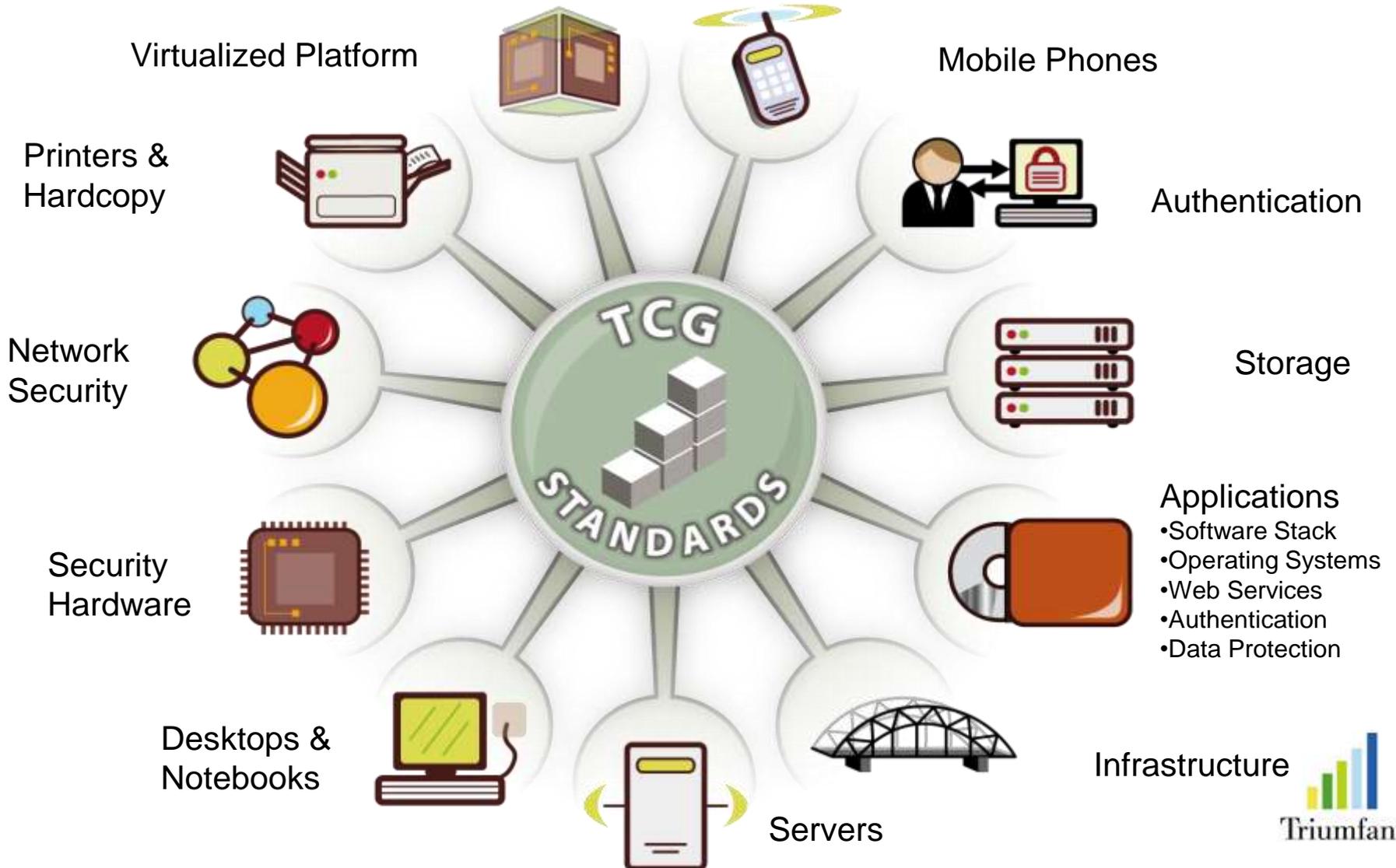
- Full set of specifications available to all
- Products shipping for more than four years

Developed by Trusted Computing Group (TCG)

- Industry standards group
- More than 100 member organizations
- Includes large vendors, small vendors, customers, etc.



TCG: Standards for Trusted Systems



Problems Solved by TNC

Network and Endpoint Visibility

- Who and what's on my network?
- Are devices on my network secure?
Is user/device behavior appropriate?

Network Enforcement

- Block unauthorized users/devices
- Grant appropriate levels of access to authorized users/devices

Device Remediation

- Quarantine and repair unhealthy devices

Network Access
Control (NAC)

Security System Integration

- Share real-time information about users, devices, threats, etc.

Coordinated
Security



Sample Network Access Control Policy

To Access the Production Network...

1. User Must Be Authenticated
 - With Identity Management System

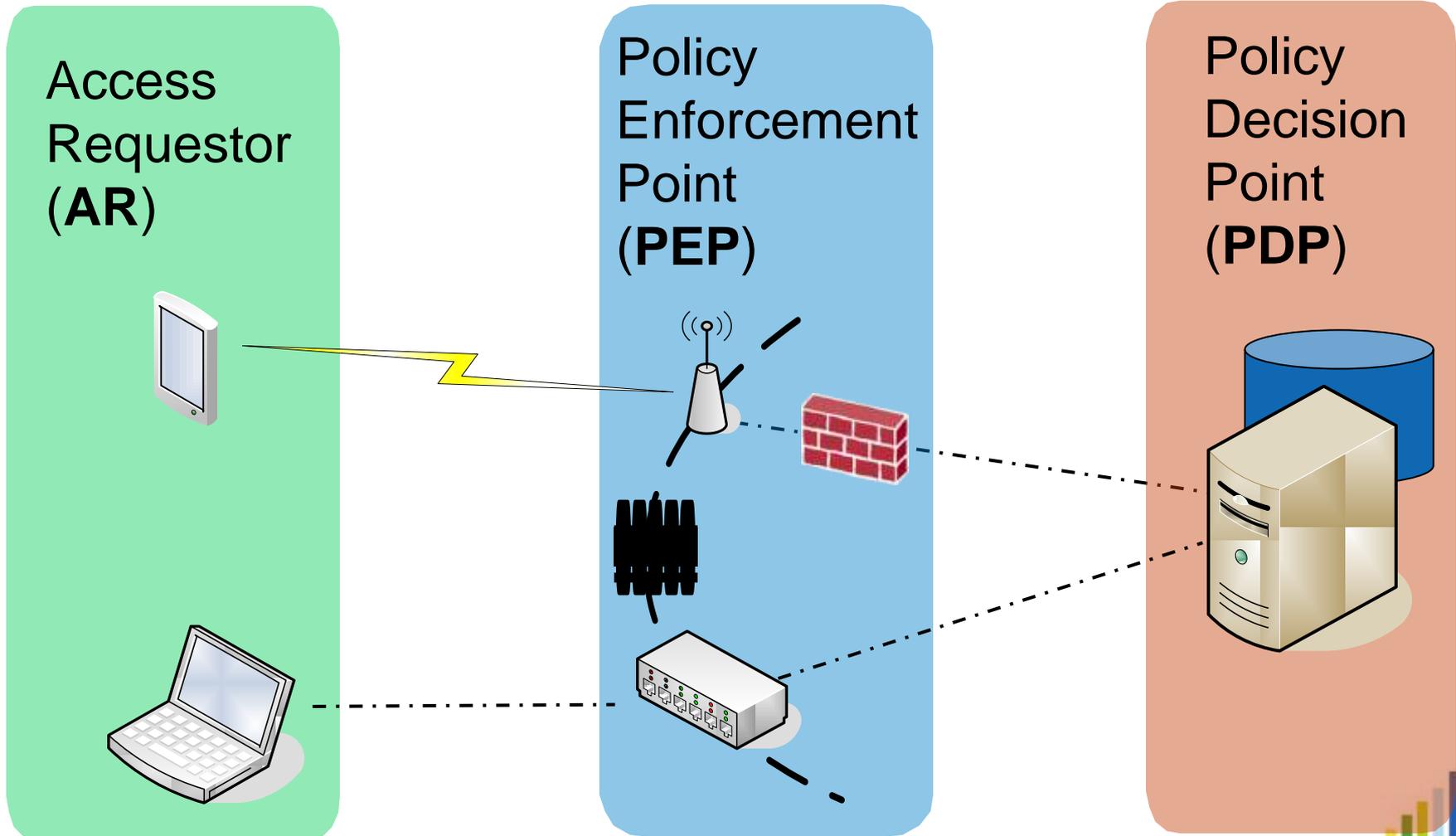
SCAP Strengths

2. Endpoint Must Be Healthy
 - Anti-Virus software running and properly configured
 - Recent scan shows no malware
 - Personal Firewall running and properly configured
 - Patches up-to-date

3. Behavior Must Be Acceptable
 - No port scanning, sending spam



Basic NAC Architecture

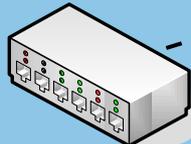


Coordinated Security

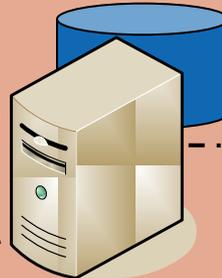
Access Requestor
(AR)



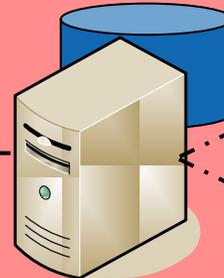
Policy Enforcement Point
(PEP)



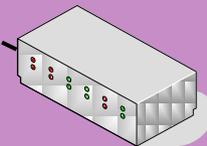
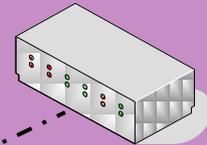
Policy Decision Point
(PDP)



Metadata Access Point
(MAP)



Sensors,
Flow
Controllers



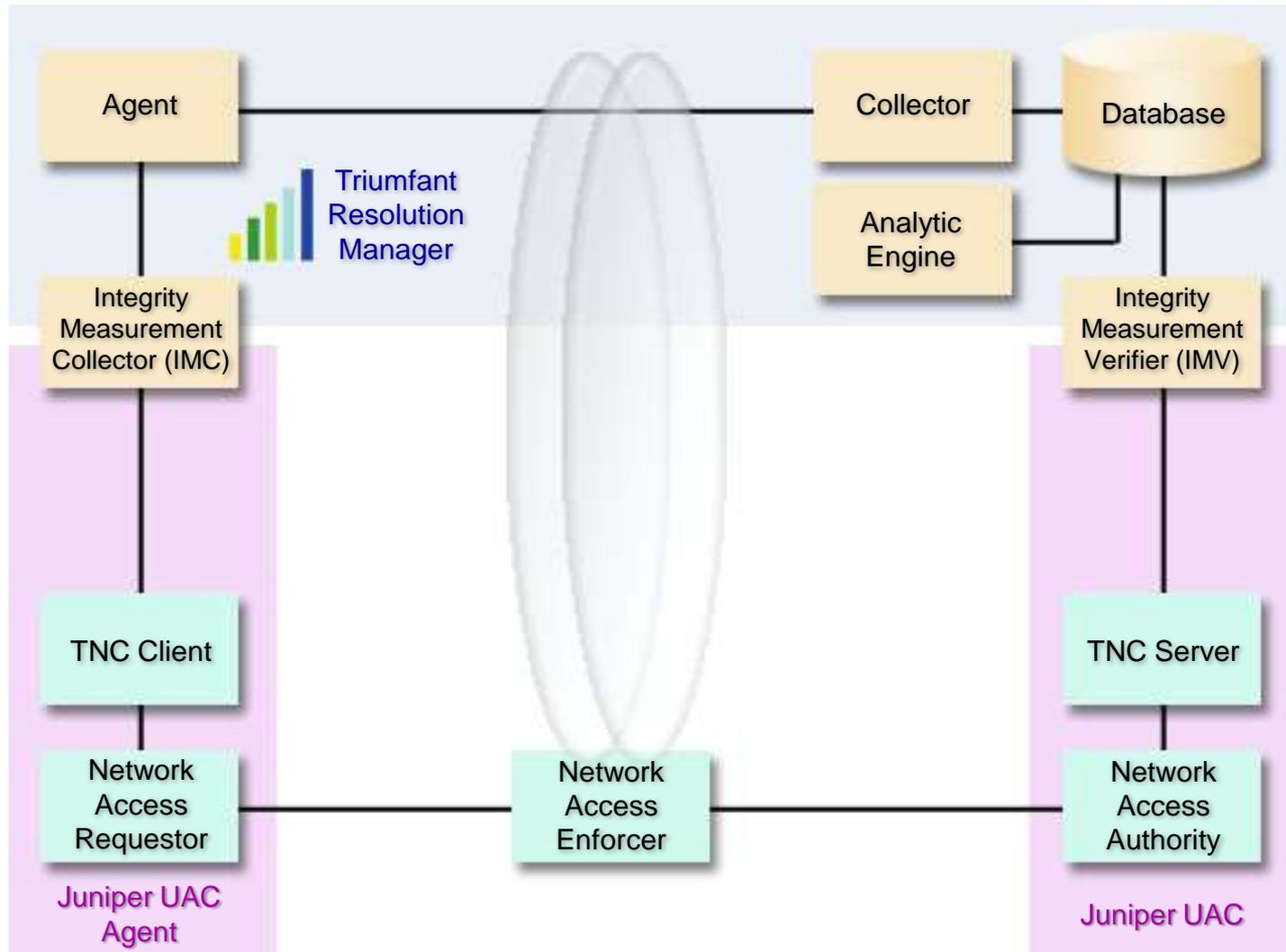
TNC and Triumfant

Triumfant's extensive data collection capabilities and its sophisticated analytic functions make it an ideal source for providing the security state information needed to make intelligent network access decisions.

- SCAP is also a logical extension, which Triumfant speaks fluently
- Triumfant keeps a current store of SCAP results, allowing for minimal intrusion to the log-in process
- Triumfant adds malware detection to the process
- Uniquely capable of automating the remediation process to restore the machine to a compliant state without human intervention



Triumphant TNC Implementation



Starting Clean and Compliant

The screenshot displays the Odyssey Access Client Manager application window. The interface is divided into a left-hand navigation pane and a main content area. The navigation pane includes sections for Adapters, Infranet Controllers, and Configuration. The main content area is currently displaying the configuration for the Ethernet adapter. The adapter is identified as a Broadcom 440x 10/100 Integrated Controller. A checkbox indicates that the Odyssey software is used to operate this adapter. The profile is set to 'ic.lab.juniper.net', and a 'Scan ...' button is available. The connection status is 'open and authenticated', with an elapsed time of 00:08:46. The network (SSID) is 'switch', and the access point is also 'switch'. The IP address is 10.0.2.50, which is highlighted by a red arrow. The packets in/out are 651 / 985. Below the connection information, the Infranet Controller status is shown as 'session established' with 09:51:14 remaining. The server is 10.0.1.5, and the compliance status is 'Your computer meets the security policies.' At the bottom of the window, there are buttons for 'Reconnect' and 'Extend Session', along with several status icons.

Odyssey Access Client Manager

File Tools Help

Adapters

- Ethernet

Infranet Controllers

- ic.lab.juniper.net

Configuration

Ethernet

Adapter: Broadcom 440x 10/100 Integrated Controller -

Use Odyssey to operate this adapter

Profile:

Connect to the network Scan ...

Connection Information

Status: open and authenticated

Elapsed time: 00:08:46

Network (SSID): switch

Access point: switch

IP address: 10.0.2.50

Packets in/out: 651 / 985

Infranet Controller

Status: session established

Session remaining: 09:51:14

Server: 10.0.1.5

Compliance: Your computer meets the security policies.

Reconnect Extend Session



IMV Test Passed

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IF-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Junos Pulse
- UAC
 - MAC Address Realms
 - Infranet Enforcer
 - Network Access
 - Host Enforcer
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

Logs

Events | User Access | Admin Access | Sensors | Client Logs | SNMP | Statistics

Log | Settings | Filters

View by filter: Standard:Standard (default) Show 200 items

Edit Query:

Update | Reset Query | Save Query...

Save Log As... | Clear Log | Save All Logs

Filter: Standard (default)

Date: Oldest to Newest

Query:

Export Format: Standard

Severity	ID	Message
Info	AUT24803	2010-09-22 11:15:01 - ic - [10.0.2.50] Renamed_Admin(Users)[NetAdmin, Remediation] - Host Checker policy 'Triumfant IMV Test' passed on host '10.0.2.50' address '00-17-08-4a-fc-b8' for user 'Renamed_Admin'.

ATTACK!

The screenshot displays a Windows XP desktop environment. In the top-left corner, the Event Viewer window is open, showing a list of events under the 'Triumphant Analysis' log. The events include several 'Information' messages and two 'Warning' messages, all dated 9/22/2010. The 'Event Properties' dialog box is open over the Event Viewer, showing details for an event: Date: 9/22/2010, Time: 10:41:20 AM, Source: Agent log, Type: Information, Event ID: 0, User: N/A, Computer: GOODLAPTOP. The description reads: 'Scan Uploaded Successfully'. Below the description, there is a link to 'http://go.microsoft.com/fwlink/events.asp'. In the bottom-left corner, the Ethernet network settings window is open, showing the adapter 'Broadcom 440x 10/100 Integrated Controller' and the profile 'ic.lab_jumper.net'. The 'Connection Information' section shows the status as 'open and authenticated' with an elapsed time of 00:19:40. The IP address is 10.0.2.50. In the center of the desktop, there is a graphic with the text 'Death by Malware' at the top, 'MALWARE' in large red letters in the middle, and 'RULES' in large red letters at the bottom. To the right of this graphic is a small skull and crossbones icon with the text 'Deathware' below it. The taskbar at the bottom shows the Start button, 'Odyssey Access Client...', 'Control Panel', and 'Event Viewer' icons. The system tray on the right shows the time as 10:47 AM.

Type	Date	Time	Source	Ci
Information	9/22/2010	10:42:08 ...	Agent log	No
Information	9/22/2010	10:42:08 ...	Agent log	No
Information	9/22/2010	10:41:20 ...	Agent log	No
Information	9/22/2010	10:40:55 ...	Agent log	No
Information	9/22/2010	10:40:55 ...	Agent log	No
Warning	9/22/2010	10:40:55 ...	Agent log	No
Warning	9/22/2010	10:40:53 ...	Agent log	No
Information	9/22/2010	10:39:55 ...	Agent log	No
Warning	9/22/2010	10:39:55 ...	Agent log	No
Information	9/22/2010	10:39:44 ...	Agent log	No
Information	9/22/2010	10:39:44 ...	Agent log	No
Information	9/22/2010	10:39:01 ...	Agent log	No
Information	9/22/2010	10:38:31 ...	Agent log	No
Information	9/22/2010	10:38:31 ...	Agent log	No
Warning	9/22/2010	10:38:31 ...	Agent log	No
Warning	9/22/2010	10:38:16 ...	Agent log	No
Information	9/22/2010	10:37:58 ...	Agent log	No

Criteria Fails, Machine Taken Off Network

The screenshot shows the Odyssey Access Client Manager application window. The title bar reads "Odyssey Access Client Manager" with standard window controls. The menu bar includes "File", "Tools", and "Help".

Left Panel:

- Adapters
 - Ethernet (selected)
- Infranet Controllers
 - ic.lab.juniper.net
- Configuration

Ethernet Section:

- Adapter: Broadcom 440x 10/100 Integrated Controller -
- Use Odyssey to operate this adapter
- Profile: ic.lab.juniper.net
- Connect to the network [Scan ...]

Connection Information:

- Status: open and authenticated
- Elapsed time: 00:04:33
- Network (SSID):
- Access point: switch
- IP address: 10.0.4.50 (indicated by a red arrow)
- Packets in/out: 355 / 518

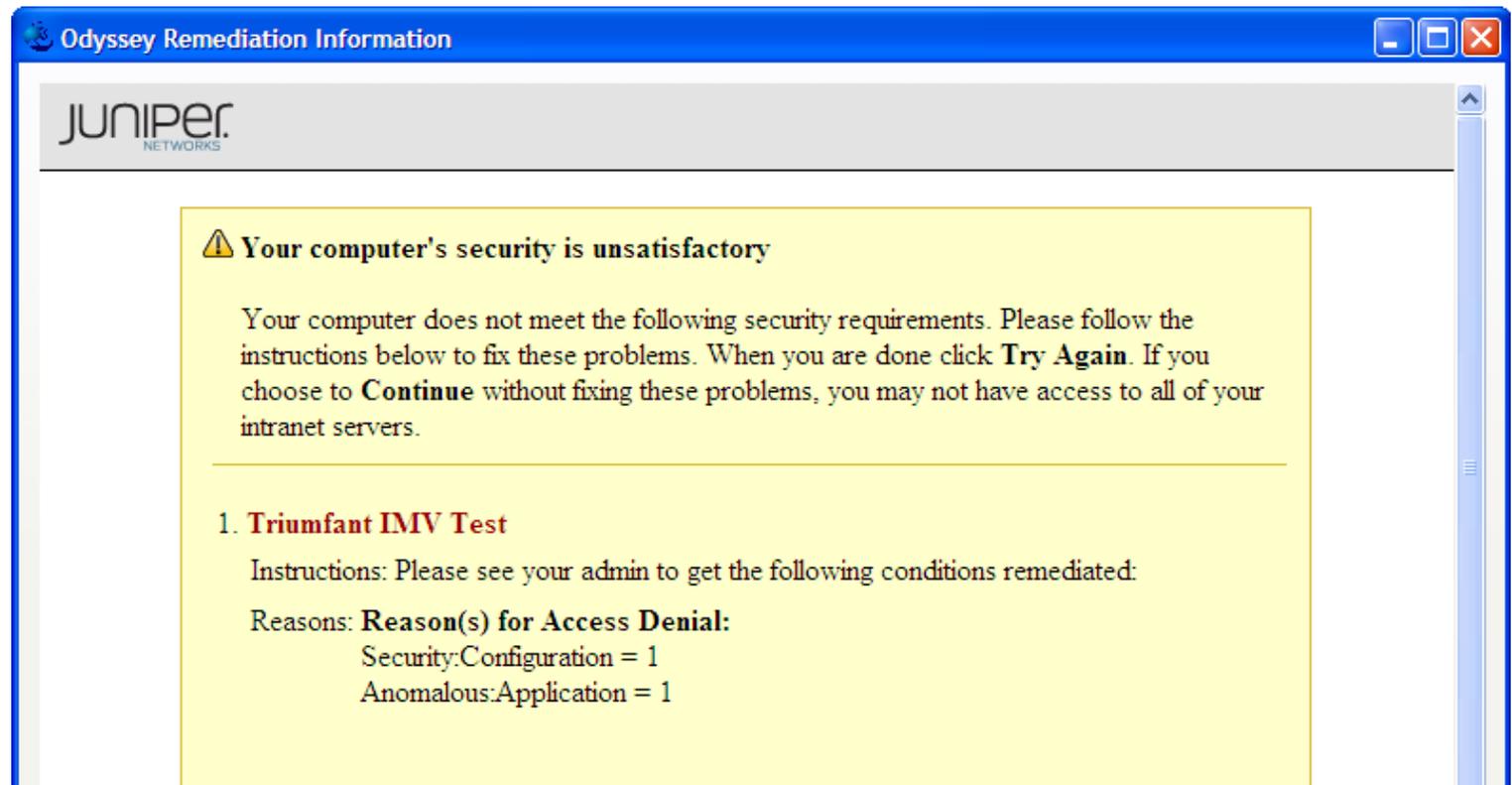
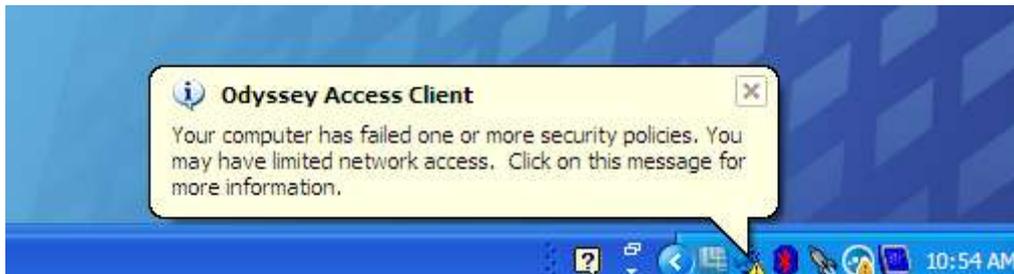
Infranet Controller:

- Status: session established
- Session remaining: 09:55:27
- Server: 10.0.1.5
- Compliance: Your computer has failed one or more security policies. You may have limited network access.
[How do I resolve this problem?](#)

Bottom Buttons: Reconnect, Extend Session, and a row of icons including a warning sign, a bar chart, a globe, and a key.



Messages to the User



Log Entry for Test Failure

JUNIPER NETWORKS

Infranet Controller Help | Guidance | Sign Out

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IF-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Junos Pulse
- UAC
 - MAC Address Realms
 - Infranet Enforcer
 - Network Access
 - Host Enforcer
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

Logs

Events | **User Access** | Admin Access | Sensors | Client Logs | SNMP | Statistics

Log | Settings | Filters

View by filter: Show items

Edit Query:

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	AUT24804	2010-09-22 11:25:15 - ic - [10.0.4.50] Renamed_Admin(Users)[Remediation] - Host Checker policy 'Triumfant IMV Test' failed on host '10.0.4.50' address '00-17-08-4a-fc-b8' for user 'Renamed_Admin' reason 'Reason(s) for Access Denial:; Security:Configuration = 1; Anomalous:Application = 1;'. Triumfant IMV Test'
Info	AUT24804	2010-09-22 11:24:15 - ic - [10.0.4.50] Renamed_Admin(Users)[Remediation] - Host Checker policy 'Triumfant IMV Test' failed on host '10.0.4.50' address '00-17-08-4a-fc-b8' for user 'Renamed_Admin' reason 'Reason(s) for Access Denial:; Security:Configuration = 1; Anomalous:Application = 1;'. Access Denial:
Info	AUT24804	2010-09-22 11:23:15 - ic - [10.0.4.50] Renamed_Admin(Users)[Remediation] - Host Checker policy 'Triumfant IMV Test' failed on host '10.0.4.50' address '00-17-08-4a-fc-b8' for user 'Renamed_Admin' reason 'Reason(s) for Access Denial:; Security:Configuration = 1; Anomalous:Application = 1;'. Access Denial:
Info	AUT24804	2010-09-22 11:22:15 - ic - [10.0.4.50] Renamed_Admin(Users)[Remediation] - Host Checker policy 'Triumfant IMV Test' failed on host '10.0.4.50' address '00-17-08-4a-fc-b8' for user 'Renamed_Admin' reason 'Reason(s) for Access Denial:; Security:Configuration = 1; Anomalous:Application = 1;'. Access Denial:
Info	EAM24805	2010-09-22 11:21:04 - ic - [0.0.0.0] Renamed_Admin(Users)[] - Radius authentication accepted for Renamed_Admin (realm 'Users') from location-group "" and attributes are: NAS-IP-Address = 10.0.1.26,NAS-Port = 13,NAS-Port-Type = 15

View Diagnosis Results



Select a 'Condition Recognized' from the Diagnosis Results Summary window to view an explanation of the condition and the supporting diagnostic evidence. To export detailed filter information to a file, select a filter and press "Save to File". Select a row and click on the "Ack/Nack" button to change the acknowledged state of a condition. Double-click on a row to see more information about the remediation status.

	Parameters	Values Selected
▶	Population Name	Demo Group
	Agent Group Name	SCAP Group
	Machine Name	goodlaptop
	Snapshot ID	178
	Snapshot Date	2010-09-22 10:47:53

Diagnosis Result Summary

	Category	Sub Category	Conditions Recognized	%Matched	Priority	Ack	Workflow Position
▶	Generic	Event	160-0 Anomalous Applicati		3	<input type="checkbox"/>	Event Reported
	Security	Configuration	File Permissions: regedit.e	50	3	<input type="checkbox"/>	New
			Unrecognized Anomalies	0	5	<input type="checkbox"/>	

Explanation

Explanation area for the selected condition. Two red arrows point from the 'Event Reported' and 'New' workflow positions in the summary table to this area.

Supporting Evidence

Files: 0	Registry: 0	Services: 0	Processes: 0	Performance: 0	Comm: 0	System: 0	Logs: 0
Unexpectedly Present: 0	Unexpectedly Absent: 0	Unknown Value: 0					

Supporting Evidence content area.

Analyze Save Analysis Email Analysis Close Event Remediate Inform Ack/Nack Save to File

View Status View Diagnosis View Changes View Snapshot Collect Snapshot << Back Finish Cancel Help

View Diagnosis Results



Select a 'Condition Recognized' from the Diagnosis Results Summary window to view an explanation of the condition and the supporting diagnostic evidence. To export detailed filter information to a file, select a filter and press "Save to File". Select a row and click on the "Ack/Nack" button to changed the acknowledged state of a condition. Double-click on a row to see more information about the remediation status.

Parameters	Values Selected
Population Name	Demo Group
Agent Group Name	SCAP Group
Machine Name	goodlaptop
Snapshot ID	183
Snapshot Date	2010-09-22 12:01:11

Diagnosis Result Summary

Category	Sub Category	Conditions Recognized	%Matched	Priority	Ack	Workflow Position
Generic	Event	166-0 Anomalous Applicati		3	<input type="checkbox"/>	Event Reported
Security	Configuration	File Permissions: regedit.e	50	3	<input type="checkbox"/>	Remediation Pendi
		Unrecognized Anomalies	0	5	<input type="checkbox"/>	

Explanation

Agent Analysis Executed: 2010-09-22 12:02:09
 Result Type: Anomalous Application
 High FrequencyStrings:
 death
 death.exe.452be13a-7868-442c-8318-1c04a4c89829.dc0ecaba-82ea-4ca0-8d95-7a46709bed95
 death.exe

Supporting Evidence

Files: 2 Registry: 1 Services: 0 Processes: 1 Performance: 0 Comm: 0 System: 0 Logs: 0

Unexpectedly Present: 2 Unexpectedly Absent: 0 Unknown Value: 0

File Name	Hash Value
%systemdrive%\documents and settings\administrator\desktop\death.exe	00088690af42870165efccdb1df3b4d
%systemdrive%\documents and settings\administrator\desktop\death.exe.452be13a-7868-442c-8318-1c04a4c89829.dc0	00088690af42870165efccdb1df3b4d

Back to the Secure Network

The screenshot shows the Odyssey Access Client Manager application window. The title bar reads "Odyssey Access Client Manager" and includes standard window controls. Below the title bar is a menu bar with "File", "Tools", and "Help".

The main interface is divided into a left sidebar and a main content area. The sidebar contains three expandable sections: "Adapters" (with a sub-item "Ethernet"), "Infranet Controllers" (with a sub-item "ic.lab.juniper.net"), and "Configuration".

The main content area is titled "Ethernet" and displays the following information:

- Adapter: Broadcom 440x 10/100 Integrated Controller -
- Use Odyssey to operate this adapter
- Profile: ic.lab.juniper.net (selected from a dropdown menu)
- Connect to the network (with a "Scan ..." button)

Below this is the "Connection Information" section, which shows:

- Status: open and authenticated
- Elapsed time: 00:07:04
- Network (SSID):
- Access point: switch
- IP address: 10.0.2.50 (highlighted with a red arrow)
- Packets in/out: 548 / 797

At the bottom of the main content area is the "Infranet Controller" section, which shows:

- Status: session established
- Session remaining: 09:52:56
- Server: 10.0.1.5
- Compliance: Your computer meets the security policies.

At the bottom of the window are two buttons: "Reconnect" and "Extend Session". To the right of these buttons are four small icons: a globe, a bar chart, a refresh symbol, and a key.



Summary

- Triumfant is fully SCAP conversant
- Triumfant's unique technology creates an equally unique SCAP capability
 - Configuration management and enforcement
 - Vulnerability management
- The Triumfant repository is an extremely useful data source for analysis and reporting
- The marriage of SCAP, TNC, and Triumfant is logical and pragmatic





Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation

September 2010